I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Secret without Reason and Costly without Accomplishment: Questioning the National Security Agency's Metadata Program

JOHN MUELLER & MARK G. STEWART*

I. INTRODUCTION

When Edward Snowden's revelations emerged in June 2013 about the extent to which the National Security Agency was secretly gathering communications data as part of the country's massive 9/11-induced effort to catch terrorists, the administration of Barack Obama set in motion a program to pursue him to the ends of the earth in order to have him prosecuted to the full extent of the law for illegally exposing state secrets.

However, the President also said that the discussions about the programs these revelations triggered have actually been a good thing: "I welcome this debate. And I think it's healthy for our democracy. I think it's a sign of maturity because probably five years ago, six years ago, we might not have been having this debate."[1]

There may be something a bit patronizing in the implication that the programs have been secret because we were not yet mature enough to debate them when they were put into place. Setting that aside, however, a debate is surely to be welcomed—indeed, much overdue. It should be conducted not only about the National Security Agency's (NSA) amazingly extensive data-gathering programs to

* John Mueller is a professor of political science at Ohio State University and a Senior Fellow at the Cato Insitute. Mark G. Stewart is a professor of engineering at the University of Newcastle, Australia.

[1] President Barack Obama, Statement by the President at the Fairmont Hotel, San Jose, California (June 7, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/06/07/statement-president.

amass information on telephone and e-mail conversations—programs that have, according to the President, included "modest encroachments" on privacy—but also more generally about the phenomenal expansion of intelligence and policing efforts in the wake of 9/11.[2]

As Dana Priest and William Arkin have documented in their remarkable book, *Top Secret America*, by 2009 there were around 1,074 federal government organizations and almost 2,000 private companies devoted to counterterrorism, homeland security, and intelligence spread over more than 17,000 locations within the country. At least 263 of these were created or reorganized after 9/11. Collectively this apparatus launched far more covert operations in the aftermath of 9/11 than it had during the entire 45 years of the Cold War.[3]

A comparison might be useful. Since 9/11, 54 cases have come to light of Islamist extremist terrorism, whether based in the United States or abroad, in which the United States itself has been, or apparently has been, targeted.[4] The total number of real terrorists, would-be terrorists, and putative terrorists populating this set of cases, excluding FBI and police undercover operatives, is around 100. Thus, the United States has created or reorganized *more than two entire counterterrorism organizations* for every terrorist arrest or apprehension it has made of people plotting to do damage within the country.

Although much of the discussion in this article can be extrapolated more widely, it focuses primarily on one of the two surveillance programs revealed by Snowden. These two programs have often been confused.[5]

One of the programs, PRISM, somewhat more commonly known as (section) 702, permits NSA to gather electronic communication

---

[2] *Id.*

[3] DANA PRIEST & WILLIAM M. ARKIN, TOP SECRET AMERICA: THE RISE OF THE NEW AMERICAN SECURITY STATE 12, 86 (2011).

[4] *See* TERRORISM SINCE 9/11: THE AMERICAN CASES (John Mueller, ed., 2014), *available at* http://politicalscience.osu.edu/faculty/jmueller/since.html.

[5] For useful discussion of the two programs, see Walter Pincus, *NSA Should Be Debated on the Facts*, WASH. POST, July 29, 2013, http://www.washingtonpost.com/world/national-security/nsa-should-be-debated-on-the-facts/2013/07/29/d57d251e-f63e-11e2-a2f1-a7acf9bd5d3a_story.html. On "known or unknown," *see In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from, No. BR 13-109 at 18, (FISC 2013). *See also* Julian Sanchez, *Decoding the Summer of Snowden*, 35 CATO POL'Y REP. 5, 1, 6-8 (2013).

information on e-mail and phone conversations after approval by a judge if the target is both outside the United States and not an American citizen and if there is an appropriate and documented foreign intelligence purpose for the collection.

The other program, known as 215, authorizes the gathering in bulk of business and communication records within the United States. It has been used in particular to amass telephone billing records—numbers called, numbers received, and conversation length—potentially for every telephone in the U.S. In principle, the 215 data are only supposed to be collected if there are "reasonable grounds to believe" the records are "relevant" to a terrorist investigation of a "known or unknown" terrorist organization or operative. Creatively expanding the word "relevant" to the breaking point, it has been taken in practice to mean that NSA can gather billing records for every telephone conversation in the country: if there might be a known or unknown needle in the haystack, the entire haystack becomes "relevant." As many, including Senator Patrick Leahy, have pointed out, this broad approach could also be applied to banking, credit card, medical, financial, and library records, all of which could be held as reasonably to be somehow "relevant" to the decidedly wide-ranging quest to catch terrorists. The information gathered by either program can be held for five years.

This article primarily deals with the more controversial 215 program, which involves the massive gathering of telephone billing records, or "metadata," within the United States. In the burgeoning debate since Snowden's revelations, a number of questions have been raised about the civil liberties and privacy implications of the NSA's massive surveillance efforts. This article focuses on three additional questions. None of these are terribly legalistic, but they are questions that ought to be given more thorough examination.

The first two—why was the program secret and how much does it cost?—never seem to come up even though they are crucial if we are going to have an adult conversation on the issue. The third—what has the program accomplished?—has attracted some attention, but it clearly needs much more, and this article examines it at some length in the broader context of the obsessive and massively expensive efforts by police and intelligence since 9/11 to deal with the threat that is envisioned to be presented by terrorism, a quest that has involved following literally millions of leads that go nowhere.[6]

---

[6] For commentary on the often-bizarre quality of this quest, see John Mueller & Mark G. Stewart, *The Terrorism Delusion: America's Overwrought Response to September 11*, 37 INT'L SEC. 1, 81–110 (Summer 2012).

Although those opposed to the program are deeply concerned about privacy issues, they have also argued that the program fails to be "an effective counterterrorism tool," in the words of Senator Leahy.[7] In December 2013, two judges came to opposite conclusions about the 215 metadata program, and it is clear the program's effectiveness figured importantly in their decisions. Judge Richard J. Leon, in finding that the program was likely unconstitutional, noted that the government "does *not* cite a single instance" in which analysis of bulk metadata collection "actually stopped an imminent attack," failed to present "any indication of a concrete danger," and provided "no proof that the program prevented terrorist attacks."[8] Eleven days later, Judge William Pauley, in approving the program, stressed in his first sentence that the world is "dangerous and interconnected" and went on to insist that the effectiveness of the data collection program "cannot seriously be disputed, " noting that the "the Government has acknowledged several successes in Congressional testimony and in declarations."[9] Meanwhile, a special Presidential group set up to review the NSA programs, while focusing mostly on legal issues, noted, in recommending the termination of 215 as currently operated, that information provided by the program "was not essential to preventing attacks and could readily have been obtained in a timely manner" and that "there has been no instance in which NSA could say with confidence that the outcome would have been different" without the program.[10]

In all this, the key question, as the Presidential review group points out, is not whether a surveillance program "makes us incrementally safer, but whether the additional safety is worth the sacrifice in terms of individual privacy, personal liberty, and public

---

[7] Ellen Nakashima, *NSA Bills Set Up A Choice in Congress: End Bulk Collection of Phone Records or Endorse It*, WASH. POST, Oct.28, 2013, http://www.washingtonpost.com/world/national-security/nsa-bills-set-up-a-choice-in-congress-end-bulk-collection-of-phone-records-or-endorse-it/2013/10/28/99007880-3fd5-11e3-a751-f032898f2dbc_story.html.

[8] Klayman v. Obama, No. 13-0851, 2013 WL 6571596, at *24 (D.D.C. Dec. 16, 2013) (emphasis in original).

[9] ACLU v. Clapper, No. 13 Civ. 3994 at *48-49 (S.D.N.Y Dec. 27, 2013), *available at* https://www.aclu.org/files/assets/order_granting_governments_motion_to_dismiss_and_denying_aclu_motion_for_preliminary_injunction.pdf.

[10] Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies 104, 119 n.119 (President's Review Grp. on Intelligence and Comm'n Tech., Dec. 12, 2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

trust."[11] The analysis in this article suggests that any benefit of the 215 metadata program is considerably outweighed by its cost even assuming that the unknown, and perhaps unknowable, cost figure is quite small. If the issue is security versus privacy, in this case, privacy wins.

II. WHY WAS THE 215 PROGRAM SECRET?

Under Executive Order 135256, classification is permitted if "disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism." The order continues: "If there is significant doubt about the need to classify information, it shall not be classified."[12] There is also a classification level of top secret. As defined in Executive Order 12356, top secret is "applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to national security."[13]

It is difficult to see how earlier exposure of the program's existence would have damaged national security, gravely or otherwise. No one seems to be saying that the Snowden documents put undercover intelligence operatives or operations overseas or elsewhere in danger of being exposed, that the documents reveal military secrets about weapons, or that they compromise United States strategy or tactics. Instead, we get such vague, atmospheric pronouncements to the press as that from outgoing FBI Director Robert Mueller in August 2013: "Mueller said that leaks by former NSA contractor Edward Snowden 'have impacted, and [are] in the process of impacting, capabilities around the world,' but when asked to expand on this, he said simply, 'No details.'"[14] Even less helpful has been the expression of "belief" promulgated by NSA chief Keith B. Alexander: "Based on what we

---

[11] *Id.* at 114.

[12] Jim Harper, John Mueller, & Mark Stewart, *Comments on Notice of Proposed Rulemaking: Passenger Screening Using Advanced Imaging Technology, TSA-2013-0004 (RIN 1652-AA67)*, CATO INSTITUTE (June 21, 2013), *available at* http://www.cato.org/sites/cato.org/files/wp-content/uploads/cato_tsa_comments.pdf.

[13] PRIEST & ARKIN, *supra* note 3 at n.10.

[14] Billy Kenber, *Outgoing Director Robert S. Mueller, III Tells How 9/11 Reshaped FBI Mission*, WASH. POST, Aug. 22, 2013, http://www.washingtonpost.com/world/national-security/outgoing-director-robert-s-mueller-iii-tells-how-911-reshaped-fbi-mission/2013/08/22/ee452170-0b54-11e3-9941-6711ed662e71_story.html.

know to date, we believe these disclosures have caused significant and irreversible harm to the security of the nation."[15]

Of course, terrorists have surely known at least since the 1990s (when Osama bin Laden ceased talking on a satellite phone) that United States intelligence is searching communications worldwide to track them down.[16] Year after year we have heard about "chatter" that has been picked up by official agencies, and one certainly must conclude that it has dawned on the chatterers that there are extensive efforts to listen in. The terrorists may not know the precise number, but they are likely to be at least dimly aware—and are unlikely to be surprised—that the NSA, in its tireless quest to conduct its global war on terror, intercepts and ingests 1.7 billion communication elements every day. These include, note Priest and Arkin, "telephone calls, radio signals, cell phone conversations, emails, text and Twitter messages, bulletin board postings, instant messages, website changes, computer network pings, and IP addresses."[17] It is possible that the current revelations will impress the terrorists even further about the extent of the surveillance effort. But even if that is so, the main effect of the revelations would be to make their efforts to communicate even more difficult and inconvenient—far more than the revelations would facilitate communication.

Conceivably, as some maintain, some exceptionally dim-witted terrorists or would-be terrorists who are oblivious to the fact that their communications are less than fully secure could exist. But such supreme knuckle-heads are surely likely to make so many mistakes—like advertising on Facebook or searching there or in chat-rooms for co-conspirators—that sophisticated and costly communications data banks are scarcely needed to track them down.[18]

Some defenders of the program have creatively argued that exposure of the 215 program has aided terrorists because they now know that NSA is gathering only metadata on telephone calls in the

---

[15] Shane Harris, *The Cowboy of the NSA*, FOREIGN POLICY (Sept. 9, 2013), http://www.foreignpolicy.com/articles/2013/09/08/the_cowboy_of_the_nsa_keith_alexander.

[16] Mary Lu Carnevale, *Tracking Use of Bin Laden's Satellite Phone*, WALL ST. J. (May 28, 2008), http://blogs.wsj.com/washwire/2008/05/28/tracking-use-of-bin-ladens-satellite-phone.

[17] PRIEST & ARKIN, *supra* note 3 at 77.

[18] *See, e.g.*, cases 16, 30, 39, 40, 41, 48, 51, and 52 in TERRORISM SINCE 9/11: THE AMERICAN CASES, *supra* note 4.

United States, not their content.[19] But, if terrorists or others read past the first paragraph in the discussions of the 215 program, they can also note that if any information gathered is deemed suspicious, investigators can apply for legal authority to record the content of the communications. They can readily do that as well in the 702 program, which gathers and monitors both metadata and content. Moreover terrorists, like many others, are likely to suspect that considerably more than metadata is gathered even under the 215 program, despite prominent denials to the contrary.

It is also argued that the program was kept secret in order to protect private communications companies, like AT&T, Verizon, and Sprint, which are dutifully supplying the NSA with data. However, the potential embarrassment of businesses, although a reasonable concern, is not usually deemed to constitute a threat, grave or otherwise, to national security and therefore fails to be a legitimate reason for classification. Moreover, it seems elemental that customers should be informed about what businesses are doing with confidential information.

Unkind people might suggest that the real reason these programs were kept secret actually stems from the administration's fear that public awareness of their "modest encroachments" on privacy would make further efforts to encroach more difficult. Thus, Reuters notes that a former Air Force secretary ominously warns that a "growing unease about domestic surveillance could have a chilling effect on proposed cyber legislation that calls for greater information-sharing between government and industry." Reuters also notes that after the revelations, more lawmakers signed on to legislation that would strengthen the privacy protections in the 1986 Electronic

---

[19] Thus, General Michael Hayden on *Meet the Press* (NBC Television Broadcast June 16, 2013) (transcript available at http://www.nbcnews.com/id/52220609/ns/meet_the_press-transcripts/t/june-lindsey-graham-saxby-chambliss-mark-udall-bobby-scott-david-ignatius-james-risen-andrea-mitchell/#.Uw-_S_ldVio): "What I fear al-Qaeda learns about this program is not what we're *allowed* to do but they learn what we're *not* allowed to do, and they learn the limits of the program." Asked on CBS' "Face the Nation" on June 30, 2013, about what harm had been done, Hayden said, "Look, we cooperate with a lot of governments around the world. They expect us to be discreet about that cooperation. I can't imagine a government anywhere on the planet who now believes we can keep a secret." *Face the Nation* (June 30, 2013) (transcript available at http://www.cbsnews.com/news/face-the-nation-transcripts-june-30-2013-hayden-olson-perkins-and-davis). Although that "harm" is a relevant concern for programs that are secret, it is scarcely relevant to the issue of why the program was made secret in the first place. Updating his opinion on "Face the Nation" on December 29, 2013, Hayden declared that the NSA had become "infinitely weaker" because of the disclosures. *Face the Nation* (CBS Television Broadcast Dec. 29, 2013) (transcript available at http://www.cbsnews.com/news/face-the-nation-transcripts-december-29-2013-hayden-drake-radack-gellman/2).

Communications Privacy Act.[20] Perhaps, then, the programs were kept secret not to protect people from terrorism, but to protect the government from the annoying and inconvenient public and Congressional outcry that constitutes the untidy stuff of democracy.

III. HOW MUCH DOES THE 215 PROGRAM COST?

If we are now to have a healthy debate about 215, NSA's massive metadata program, it seems reasonable to suggest that debaters should be supplied with information about how much the program costs. This information would furnish a key starting point for any debate.

Presumably, that figure has thus far been classified because the program itself was classified. But now that we know only too well that the program exists, why should its cost remain secret? It is difficult to see how knowing that cost would help the terrorists.

It is possible, however, that the figure for the program remains undisclosed in part because no one actually knows how much the program costs. Priest and Arkin suggest that this phenomenon is widespread. In researching their book, they discovered that the spending increases on counterterrorism in the aftermath of 9/11 often took place so fast and so chaotically that no one was able to track the costs.[21]

A. *Program, Investigatory, and Opportunity Costs*

The direct costs of maintaining the 215 program might be quite low. However, a full accounting should include not only the actual cost of gathering and storing the surveillance data, but also the costs of constantly sorting through it to generate and develop leads. According to the NSA's director of compliance, the agency queries its databases about 20 million times each month.[22] Presumably that includes both databases and involves a great deal of human interaction, all of which must be paid for.

---

[20] Andrea Shalal-Esa & Joseph Menn, *U.S. Domestic Spying Controversy Complicates Cybersecurity Efforts*, REUTERS, June 8, 2013, http://www.reuters.com/article/2013/06/08/us-usa-security-cyberpolicy-analysis-idUSBRE95702R20130608.

[21] PRIEST & ARKIN, *supra* note 3, at xviii-xix.

[22] Charlie Savage, *N.S.A. Calls Violations of Privacy 'Minuscule,'* N.Y. TIMES, Aug. 16, 2013 at A12.

Costs should also include those involved in following up the leads once they have been generated, discussed in the next section of this article.

Opportunity costs should also be included in the tally: what else could the money have been used for? For example, it has often been noted that the FBI and other agencies have downgraded other priorities, including the pursuit of white collar crime like fraudulent banking practices, to focus on the pursuit of (mostly nonexistent) terrorists. To fully evaluate the costs of the NSA surveillance efforts, one would need to take this into account.

B. *Privacy Costs: The Issue of Trust*

In addition, some consideration should be made for the less quantifiable costs of privacy invasion and for the potential misuse of the data. Although the program has built-in safeguards, its operation ultimately requires us to trust those in charge. Citing historical precedents from the days of Richard Nixon and J. Edgar Hoover and from the runup to the Iraq War of 2003, Stephen Walt has suggested (or warned) that the program could be used to intimidate or harass whistle-blowers, dissidents, and overly-inquisitive journalists: "once someone raises their head above the parapet and calls attention to themselves by challenging government policy, they can't be sure that someone inside government won't take umbrage and try to see what dirt they can find."[23]

That officials have several times been caught in lies—or supreme exercises in Clintonian sophistry—about the NSA programs scarcely proves that NSA information will be abused, but it certainly enhances the wariness about the programs.

There is, for example, the response of NSA director Alexander to a March 2012 cover story in *Wired* magazine that reported the views of William Binney, a former NSA official who contended that, without a warrant, the NSA was collecting "a vast trove of international and domestic billing records" from major American telephone companies and that "they're storing everything they gather."[24] In the ensuing months, Alexander blithely denied Binney's contention. "To think

---

[23] Stephen Walt, *The Real Threat Behind the NSA Surveillance Programs*, FOREIGN POLICY (June 10, 2013), http://www.foreignpolicy.com/posts/2013/06/10/what_me_worry_the_real_threat_behind_the_nsa. *See also* Sanchez, *supra* note 5.

[24] James Bamford, *The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)*, WIRED.COM:THREAT LEVEL (Mar. 15, 2012), http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter.

we're collecting on every US person. . . that would be against the law. . . The fact is we're a foreign intelligence agency."[25] He also categorically insisted that "we don't hold data on U.S. citizens," a statement that has been defended by the administration on the grounds that the NSA's internal definition of "data" does not include "metadata"—a language-stretching nuance Alexander neglected to mention when he made his statement. As it happens, however, the agency's actual internal definition of "data" *does* specifically include "call event records and other Digital Network Intelligence metadata."[26]

Then, in March 2013, Director of National Intelligence James Clapper was asked by Senator Ron Wyden in a Senate Intelligence Committee hearing, "Does the NSA collect any type of data at all on millions or hundred of millions of Americans?" Even knowing that Wyden, due to his position on the committee, knew what the answer to that question was, Clapper blandly demurred: "No, sir. . . Not wittingly." Wyden says he had sent the question to Clapper's office the day before and that Clapper was also given a chance later to amend his answer. After Snowden's revelations three months later spectacularly shattered Clapper's crisp denial (as well as Alexander's earlier ones), Clapper sent a letter to the Committee stating that his answer had been "clearly erroneous" and that when responding he imagined that the question referred to content, not metadata which he somehow believed the NSA does not collect "wittingly." Clapper has also said that an honest response would have required him to divulge secrets that were highly classified, and thus he came up with the "least untruthful" answer he could imagine at the time.[27]

There is additional evidence of deception in the disclosure that the NSA illegally collected email content data on thousands, or tens of thousands, of Americans before that practice was closed down by the courts in 2011.[28] The court's opinion on this was classified, and the

---

[25] James Bamford, *They Know Much More Than You Think*, N.Y. REV. OF BOOKS, Aug. 15, 2013, http://www.nybooks.com/articles/archives/2013/aug/15/nsa-they-know-much-more-you-think/.

[26] Barton Gellman, *NSA Broke Privacy Rules Thousands of Time Per Year, Audit Finds*, WASH. POST, Aug. 15, 2013, http://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html.

[27] Eugene Robinson, *We Can Handle the Truth on NSA Spying*, WASH. POST, July 4, 2013, http://www.washingtonpost.com/opinions/eugene-robinson-we-can-handle-the-truth-on-nsa-spying/2013/07/04/76ef2c92-e408-11e2-a11e-c2ea876a8f30_story.html. *See also* Bamford, *supra* note 25.

[28] Ellen Nakashima, *NSA Gathered Thousands of Americans' E-mails Before Court Struck Down Program*, WASH. POST, Aug. 21, 2013,

Obama administration fought a Freedom of Information lawsuit seeking to get it released.[29] In the wake of the Snowden disclosures, however, the opinion was finally declassified and released in heavily redacted form. In it, the judge specifically points out that he had previously been the victim of "a substantial misrepresentation regarding the scope of a major collection program" and that the information gathered had been "fundamentally different from what the court had been led to believe."[30]

Similar concerns were raised in a 2009 ruling that had originally been classified as top secret dealing with the way the NSA probed phone numbers on an "alert list." When it was finally declassified under pressure in 2013, the ruling included declarations that the government had failed to comply with the court's orders and had compounded this by "repeatedly submitting inaccurate descriptions of the alert process" and that court-approved privacy safeguards had "been so frequently and systematically violated" that they "never functioned effectively." A senior official explained rather lamely, but entirely plausibly, that any violations were "unintentional" because "there was nobody at N.S.A. who really had a full understanding of how the program was operating at the time."[31]

It might be wondered what *intentional* violations could lead to, keeping Walt's admonition in mind. Senator Dianne Feinstein, who chairs the Senate Intelligence Committee, insists that her committee "has never identified an instance in which the NSA has intentionally abused its authority to conduct surveillance for inappropriate purposes." However, the agency's director of compliance has indicated that there have been a very small number (perhaps one every five years) of "willful errors."[32]

The disclosure that in 2006 the NSA deliberately weakened an encryption standard accepted both nationally and internationally in a systematic effort to defeat privacy protections for Internet communications, a venture that compromised the National Institute

---

http://www.washingtonpost.com/world/national-security/nsa-gathered-thousands-of-americans-e-mails-before-court-struck-down-program/2013/08/21/146ba4b6-0a90-11e3-b87c-476db8ac34cd_story.html. *See also* Charlie Savage & Scott Shane, *Secret Court Rebuked N.S.A. on Surveillance,* N.Y. TIMES Aug. 22, 2013 at A1.

[29] Gellman, *supra* note 26.

[30] Nakashima, *supra* note 28.

[31] Scott Shane, *Court Upbraided N.S.A. on Its Use of Call-Log Data*, N.Y. TIMES, Sept. 10, 2013, at A14.

[32] Savage, *supra* note 22.

of Standards and Technology in the process, is relevant as well to a discussion of credibility.[33]

In all this, an assessment of the privacy costs attendant on the NSA's surveillance efforts should hold in mind, to the degree to which they apply, warnings about an intimidation factor is suggested in this passage from George Orwell's novel, *1984*:

> There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.[34]

III. WHAT HAS THE 215 PROGRAM ACCOMPLISHED?

Once one knows the cost of the program, one is in a position to weigh that figure against the benefit the program has generated. The President insists that the privacy-encroaching programs "help us prevent terrorist attacks" and therefore "on net, it was worth us doing."[35] However, they are worth us doing only if their benefit, on net, outweighs their cost—if any gains in security are enough to justify the privacy and other costs.[36] And that is a calculation that should be made, not simply declared.

A. *The 9/11 Atmosphere: Consequences and Persistence*

To begin an appraisal of this issue, one must assess the program in context. It has been only one cog in the massive intelligence-gathering machine impelled by the trauma of 9/11. The trauma is certainly

---

[33] Shane, *supra* note 31; Sanchez, *supra* note 5.

[34] Bamford, *supra* note 25.

[35] Statement by the President at the Fairmont Hotel, *supra* note 1.

[36] For an introduction to this process with specific applications to counterterrorism policy, see JOHN MUELLER & MARK G. STEWART, TERROR, SECURITY, AND MONEY: BALANCING THE RISKS, BENEFITS, AND COSTS OF HOMELAND SECURITY (2011).

understandable. But the fears, and therefore the hasty and expensive actions they inspired, have been substantially inflated. As anthropologist Scott Atran puts it, "Perhaps never in the history of human conflict have so few people with so few actual means and capabilities frightened so many."[37]

In the immediate aftermath of the September 11 attacks, recalls Rudy Giuliani, who was mayor of New York at the time, "anybody, any one of these security experts, including myself, would have told you on September 11, 2001, we're looking at dozens and dozens and multiyears of attacks like this."[38] Such fears and concerns were plausible extrapolations from the facts then at hand. However, that *every* "security expert" should hold such erroneous views is fundamentally absurd. It was also an entirely plausible extrapolation from facts then at hand that 9/11 could prove to be an aberration rather than a harbinger.[39] Yet it appears that no one in authority could even imagine that proposition to be true even though it could have been taken to fit the available information fully as well as the passionately-embraced alarmist perspective. At any rate, operating under that apparently unanimous mentality, US intelligence extravagantly imagined that the number of trained al-Qaeda operatives in the United States was between 2,000 and 5,000.[40]

Over the years, such thinking has been internalized and institutionalized in a great many ways, and it has proved to be notably resistant to counter-information. Indeed, officials often seem to live in what might be called "I think, therefore they are" denial.[41] Thus, on February 11, 2003, a year and a half after 9/11, FBI Director Robert Mueller assured the Senate Intelligence Committee that "the greatest

---

[37] SCOTT ATRAN, TALKING TO THE ENEMY: FAITH, BROTHERHOOD, AND THE (UN)MAKING OF TERRORISTS (2010), xiv. *See also* JOHN MUELLER, OVERBLOWN (2006); Mueller & Stewart *supra* note 6.

[38] Miles O'Brien & Carol Costello, *Giuliani:'Have to Be Relentlessly Prepared,'* CNN (July 22, 2005), http://www.cnn.com/2005/US/07/22/giuliani.

[39] John Mueller, *Harbinger or Aberration?* NATIONAL INTEREST, Sept.1, 2002, at 45; John Mueller, *False Alarms*, WASH. POST, Sept. 29, 2002, http://politicalscience.osu.edu/faculty/jmueller//WPFALSE.PDF; Russell Seitz, *Weaker Than We Think*, AMERICAN CONSERVATIVE, Dec. 6, 2004, http://www.theamericanconservative.com/articles/weaker-than-we-think/.

[40] Bill Gertz, *5,000 in U.S. Suspected of Ties to al Qaeda; Groups Nationwide Under Surveillance,* WASH. TIMES, July 11, 2002; and Richard Sale, *US al Qaida Cells Attacked,* UPI (Oct. 31, 2002), http://www.upi.com/Top_News/2002/10/31/UPI-Special-US-al-Qaida-cells-attacked/UPI-75381036108294.

[41] *See* Mueller & Stewart, *supra* note 6.

threat is from al-Qaeda cells in the US that we have not yet identified." He somehow judged the threat from those unidentified entities to be "increasing" and claimed to know that al-Qaeda "maintains the ability and the intent to inflict significant casualties in the US with little warning."[42] On February 16, 2005, he testified before the same committee that he remained "very concerned about what we are not seeing," a sentence rendered in bold lettering in his prepared text.[43] By that time, however, an FBI report had concluded that, despite years of well-funded sleuthing, it had yet to uncover a single true al-Qaida sleeper cell in the United States.[44]

Since the number of al-Qaeda operatives actually in the country came out to be zero or nearly so, and since the threat of terrorism in the country proved to be far more limited than initially feared—not even one of the "dozens and dozens" of attacks like 9/11 ever materialized of course—there might logically have been some judicious cutbacks to the funds devoted to dealing with the issue in subsequent years. Far overdue, clearly, are extensive and transparently-presented studies seeking rationally to evaluate the massive increases in homeland security expenditures that have taken place since 9/11—increases that total well over $1 trillion. But virtually none of this has been done by the administrators in charge.[45] Instead initial, if clearly alarmist, perspectives have substantially been maintained and vast and hasty increases in spending on homeland security continue to be perpetuated.

Important in this have been increases in intelligence and policing as the questing enterprise, central to which is the NSA, continues to be expanded, searching for the needle by adding more and more hay.

In the process, information has been folded into a "Threat Matrix," an itemized catalogue of all the "threats"—or more accurately "leads"—needing to be followed up. As Garrett Graff explains, the

---

[42] *Testimony before the Senate Select Committee on Intelligence of the United States Senate* (Feb. 11, 2003) (testimony of Robert S. Mueller, III, Director, Federal Bureau of Investigation), *available at* https://www.fas.org/irp/congress/2003_hr/021103mueller.html.

[43] *Testimony before the Senate Select Committee on Intelligence of the United States Senate* (Feb. 16, 2005) (testimony of Robert S. Mueller, III, Director, Federal Bureau of Investigation), *available at* http://www.fbi.gov/news/testimony/global-threats-to-the-u.s.-and-the-fbis-response-1.

[44] Brian Ross, *Secret FBI Report Questions Al Qaeda Capabilities: No 'True' Al Qaeda Sleeper Agents Have Been Found in U.S.*, ABC NEWS (Mar. 9, 2005), http://abcnews.go.com/WNT/Investigation/story?id=566425.

[45] For a discussion, *see* MUELLER & STEWART, *supra* note 36 at 1-9.

government pursues "upwards of 5,000 threats per day."[46] Impelled by what some have called "The 9/11 Commission Syndrome"—an obsession with the career dangers in failing "to connect the dots"—it is in no one's interest to cull the threats "because it was possible you'd cull the wrong threat and end up, after the next attack, at the green felt witness table before the next congressional inquiry."[47] Consequently, the Threat Matrix "tracks all the unfolding terrorist plots and intelligence rumors" and is "filled to the brim with whispers, rumors, and vacuous, unconfirmed information."[48] In result, "claims that ordinarily wouldn't have made it past the intake agent, claims that wouldn't even be written down weeks earlier, suddenly became the subject of briefs to the President in the Oval Office."[49] Graff supplies an example. One entry in the Threat Matrix is crisply cited as "a threat from the Philippines to attack the United States unless blackmail money was paid." It turns out that this entry was based on an e-mail that said, "Dear America. I will attack you if you don't pay me 99999999999999999999999999999999999999999 dollars. MUHAHAHA."[50]

If, aided by the Threat Matrix, the government pursues some 5000 "threats" or leads each day, and if each lead takes an average of a half a week to investigate, the FBI has pursued some six million or more of them over the years since 9/11—a process that has led to, at the very most, a few hundred prosecutions, most of them on minor charges.[51]

Moreover, whatever the ratio of needle to hay, living with the Threat Matrix seems to take a psychological toll on its daily readers. As Graff vividly describes the process, the Threat Matrix comes off as "a catalogue of horrors," as the "daily looming prognoses of Armageddon," and as "a seeming tidal wave of Islamic extremist anger that threatened to unhinge American society," and it could become

---

[46] GARRETT M. GRAFF, THE THREAT MATRIX: THE FBI AT WAR IN THE AGE OF GLOBAL TERROR 399 (2011).

[47] *Id.* at 400.

[48] *Id.* at 344, 345.

[49] *Id.* at 344.

[50] *Id.* at 398. Graff reports that the FBI dutifully ran down the e-mail's author and sent information to Philippine police who then paid a visit to the would-be extortionist's parents.

[51] CENTER ON LAW AND SECURITY, TERRORISM TRIAL REPORT CARD: SEPTEMBER 11, 2001-SEPTEMBER 11, 2009 (2010), *available at* http://www.lawandsecurity.org/Portals/0/documents/02_TTRCFinalJan142.pdf.

"all-consuming and paralyzing"—as one reader puts it, "Your mind comes to be dominated by the horrific consequences of low-probability events."[52] In essence, it is like being barricaded in an apartment and listening only to the police radio for information about what is going on outside. Or one reader offers another comparison: "Reading the Threat Matrix every day is like being stuck in a room listening to loud Led Zeppelin music," and, after a while, you begin to suffer from "sensory overload" and become "paranoid" about the threat."[53] Recalls former CIA Director George Tenet, "You could drive yourself crazy believing all or even half of what was in it."[54]

As Jack Goldsmith, another reader, stresses, "It is hard to overstate the impact that the incessant waves of threat reports have on the judgment of people inside the executive branch who are responsible for protecting American lives." He quotes Tenet, "You simply could not sit where I did and read what passed across by desk on a daily basis and be anything other than scared to death about what it portended." This, writes Goldsmith, captures "the attitude of every person I knew who regularly read the threat matrix."[55] *Every* person.

Goldsmith's account suggests that the sheer number of "threats," combined with the fact that these scarcely ever lead to anything, never inspired analysts and policymakers to consider the rather plausible, if arguable, conclusion that there was little or nothing out there to fear. Rather, it caused them—exclusively it seems—to embrace the dead opposite: "The want of actionable intelligence combined with a knowledge of what might happen produced an aggressive, panicked attitude that assumed the worst about threats."[56] George Tenet agrees when he talks about "the palpable fear that we felt on the basis of the fact that there was so much we did not know.[57] "Present fears," observes Macbeth, "are less than horrible imaginings." Or, in today's lingo, "Absence of evidence is evidence of existence."

---

[52] GRAFF, *supra* note 46 at 19, 489, 345, 400.

[53] JACK GOLDSMITH, THE TERROR PRESIDENCY: LAW AND JUDGMENT INSIDE THE BUSH ADMINISTRATION 72 (2007).

[54] GEORGE TENET, AT THE CENTER OF THE STORM: MY YEARS AT THE CIA 232 (2007).

[55] GOLDSMITH, *supra* note 53 at 72.

[56] *Id.* at 74.

[57] *60 Minutes* (CBS Television Broadcast Apr. 25, 2007), *available at* http://www.cbsnews.com/news/george-tenet-at-the-center-of-the-storm.

B. *The NSA: Efforts and Accomplishments*

In the panicky aftermath of 9/11, the National Security Agency, the institution of central concern here, has also expanded massively, and its computerized surveillance programs have been a central part of that process. As of 2011, the floor space it occupied matched that of the Pentagon.[58]

It is important to evaluate what these programs have accomplished in order to determine whether "on net" they have been "worth us doing" in their central mission of countering terrorism.

When asked in June 2013 at Senate hearings if NSA's massive data-gathering programs were "crucial or critical" in disrupting terrorist threats, the agency's head, General Keith Alexander, doggedly testified that in "dozens" of instances the databases "helped" or were "contributing"—though he did seem to agree with the word "critical" at one point.[59] The key issue for evaluating the programs, however, given their costs and privacy implications, would be to determine not whether the huge databases were helpful or contributing, but whether they were necessary.[60]

After his testimony, Alexander provided Congress a list of terrorism cases in which his surveillance measures had helped to disrupt terrorist plots or to identify suspects. The list reportedly numbers 54—unsurprisingly, the list itself is classified. On the surface, this seems to be an amazingly small number for several years' work. There have been hundreds of terrorism cases in the United States since 9/11. Some 54 of these, as noted earlier, have led to full-bore prosecutions for plotting to attack targets in the United States.[61] There are dozens more that have led to prosecutions for sending or plotting to send support to terrorists overseas, while a few hundred have involved terrorism investigations that led to prosecutions on lesser charges. There have also been hundreds—or perhaps even

---

[58] PRIEST & ARKIN, *supra* note 3 at 74.

[59] *Senate Investigates NSA Leak*, CNN Newsroom (CNN Television Broadcast June 12, 2013) (transcript available at http://transcripts.cnn.com/TRANSCRIPTS/1306/12/cnr.11.html).

[60] NSA operatives sometimes suggest the program "ultimately completes the picture" or, in the words of FBI Deputy Director Sean Joyce, "closes the gap" on information on a case. These formulations ingeniously, if deceptively, create the impression that the information was necessary. Ellen Nakashima, *NSA Cites Case as Success of Phone Data-Collection Program*, WASH. POST, Aug. 8, 2013,http://www.washingtonpost.com/world/national-security/nsa-cites-case-as-success-of-phone-data-collection-program/2013/08/08/fc915e5a-feda-11e2-96a8-d3b921c0924a_story.html.

[61] *See* in TERRORISM SINCE 9/11: THE AMERICAN CASES, *supra* note 4.

thousands—of terrorism cases overseas outside of war zones. If the NSA programs were so valuable, one would think that investigators on just about every case would routinely run their information by the NSA. The exercise would be helpful even if the NSA comes up blank because that would allow investigators to close off some avenues of potential investigation that, if pursued, would have proven to be a waste of time and effort, allowing them to follow leads more likely to be productive.

An examination of public information on the terrorism cases in the United States suggests that investigators and prosecutors have not done so.[62] This could be taken to suggest, perhaps, either that they have only occasionally found the NSA to be a helpful ally or that they were afraid that if they queried the NSA on the case at hand, the agency would spew out a raft of leads that would unproductively clutter and distract their investigation while greatly increasing its costs.

The experience at the FBI with NSA leads may be suggestive here. Explains Walter Pincus, if operatives at NSA, sorting through their 215 metadata collection or other sources, uncover "a questionable pattern" such as "calls to other suspect phones," they send a report to the FBI for investigation.[63] At NSA this process has sometimes been called "We Track 'Em, You Whack 'Em."[64] The FBI, then, is routinely supplied with what Graff calls "endless lists of 'suspect' telephone numbers." When followed up, these "leads" virtually never go anywhere: of 5000 numbers passed along, only 10—two-tenths of one percent—"panned out enough for the bureau to bother" to get court permission to follow them up. At the FBI, the NSA tips are often called "Pizza Hut" leads because, following them up, FBI agents "inevitably end up investigating the local pizza delivery guy." There is, in other words, not much of anything to "whack." At one point, the generally diplomatic Robert Mueller bluntly told NSA director Alexander, "You act like this is some treasure trove; it's a useless time suck." An agent in the trenches puts it a bit less delicately: "You know how long it takes to chase 99 pieces of bullshit?"[65]

---

[62] *See, e.g.*, the case studies in TERRORISM SINCE 9/11: THE AMERICAN CASES, *supra* note 4.

[63] Pincus, *supra* note 5.

[64] Dana Priest, *NSA Growth Fueled by Need to Target Terrorists*, WASH. POST, July 21, 2013, http://www.washingtonpost.com/world/national-security/nsa-growth-fueled-by-need-to-target-terrorists/2013/07/21/24c93cf4-f0b1-11e2-bed3-b9b6fe264871_story.html.

[65] GRAFF, *supra* note 46 at 527.

C. *The Cases*

According to the testimony of an NSA official, of the 54 cases that were supposedly disrupted by NSA surveillance data, more than 90 percent involved information from the 702, or PRISM, program which allows the NSA to intercept communications by targets abroad after obtaining judicial approval.[66] Thus, the 215 program, in which metadata are accumulated and stored for all telephone calls within the United States, presumably played a role only in around 5 cases over the course of the program. According to General Alexander, only 13 of the 54 cases on the classified list had a "homeland nexus," the others having occurred in Europe (25), in Asia (11), and in Africa (5).[67]

Four of the cases, all presumably included in the "homeland nexus" subset, were publically discussed in Congressional testimony on June 18, 2013, by Alexander and by Sean Joyce, Deputy Director of the FBI.[68] Insofar as NSA surveillance played a role at all in these cases, it seems that, in almost all cases, it was the 702 program, not the 215 one, that was relevant.[69]

Although the full array of cases remains classified, Senator Patrick Leahy has said that the notion that these cases represent disrupted

---

[66] Pincus, *supra* note 5.

[67] Peter Finn, *NSA Chief Says Surveillance Programs Helped Thwart Dozens of Plots*, WASH. POST, June 27, 2013, http://www.washingtonpost.com/world/national-security/nsa-chief-says-surveillance-programs-helped-thwart-dozens-of-plots/2013/06/27/e97ab0a2-df70-11e2-963a-72d740e88c12_story.html.

[68] A related justification for the data storage program holds that, if it had been in place in 2001, it could have led to finding the location of one of the 9/11 hijackers who was calling a safe house in Yemen from San Diego. This instance plays an important role in Judge Pauley's "Memorandum & Order" of December 2013 upholding the surveillance programs. However, insofar as this justification is valid, it would have been the 702 program that was relevant, not the 215 program. Moreover, the CIA already was tracking the man's communications and knew he had entered the United States. It also knew about the calls to the safe house, but failed to trace the calls even though it had both the ability and authority to do so. It did not need a vast data bank. Michael German, *No NSA Poster Child: The Real Story of 9/11 Hijacker Khalid al-Mihdhar*, DEFENSE ONE (Oct. 16, 2013), http://www.defenseone.com/ideas/2013/10/no-nsa-poster-child-real-story-911-hijacker-khalid-al-mihdhar/72047/?oref=d-interstitial-continue. Justin Elliott, *Judge on NSA Case Cites 9/11 Report, But It Doesn't Actually Support His Ruling*, PROPUBLICA (Dec. 28, 2013), http://www.propublica.org/article/fact-check-the-nsa-and-sept-11.

[69] Carlo Muñoz, *NSA Chief Cites 50 Foiled Plots in Defense of Spying Programs*, THE HILL (June 18, 2013), http://thehill.com/homenews/house/306381-nsa-chief-cites-50-foiled-plots-in-defense-of-spying-programs.

plots is "plainly wrong." Indeed, "they weren't all plots and they weren't all thwarted."[70]

Only one, it appears, relied on the 215 program in any significant way.[71] It is among the four disclosed ones, and it involves a San Diego cab driver from Somalia who has been convicted of sending the decidedly non-princely sum of $8,500 to help a designated terrorist group in Somalia fight Ethiopians who, with US support, had recently invaded the country. The government had been tapping his telephone for months, and Director Mueller appears to have singled out this case as the only one in which the collection of phone data had been "instrumental," a word, of course, that is not as strong as "crucial" or "critical" or "necessary."[72] Joyce says that an investigation of the potential case using 215 information that began in October 2007 "did not find any connection to terrorist activity," but that there was a breakthrough when NSA connected a San Diego number with a suspicious contact outside the country using 215.[73] However, it is not clear they needed data bank to sort through. Says Senator Ron Wyden, investigators had all the information they needed to get a court order to investigate.[74]

A correspondent for *The Hill* breathlessly characterizes the cab driver culprit as "a top terrorist financier in San Diego, who was supporting militant extremist groups in Somalia."[75] However, it certainly appears that the crime prosecuted at great effort and cost was, overall, a rather trivial one.

The second disclosed case seems to be even more trivial. It involves three Muslim men, all naturalized American citizens, one in Kansas City and two in New York. At the time of the American invasion of Iraq in 2003, they decided they needed to fight for their "faith and community," in the words of one of them. Four years later,

---

[70] German, *supra* note 68.

[71] *Id;* Sean Vitka, *The Dragnet's Day in Court*, SLATE (Sept. 30, 2013), http://www.slate.com/articles/technology/future_tense/2013/09/basaaly_moalin_s_defense_team_takes_on_mass_nsa_telephone_surveillance.html.

[72] Ken Dilanian, *NSA Faces Backlash Over Collecting Phone Data*, L.A. TIMES, July 27, 2013, http://articles.latimes.com/2013/jul/27/nation/la-na-nsa-politics-20130728.

[73] Tom McCarthy, *NSA Chief Says Exposure of Surveillance Programs Has 'Irreversible' Impact–As It Happened,* THE GUARDIAN (June 18, 2013), http://www.theguardian.com/world/2013/june/18/nsa-chief-house-hearing-surveillance-live.

[74] Nakashima, *supra* note 60.

[75] Muñoz, *supra* note 69.

one of the men was able to connect to two apparently experienced al-Qaeda operatives in Yemen. Hoping to join the fight in Iraq, Afghanistan, or Somalia, the American men sent money and equipment to their new friends in Yemen under the impression that these would be set aside for their military training. Over several months they sent thousands of dollars—one of them says it totaled more than $23,000—as well as watches, cold-weather gear, some Garmin GPS units, and a remote-controlled toy car. However, the recipients divided the physical loot among themselves and spent the money on (real) cars and as awards to families of Islamic martyrs. In 2008, the scam artists requested further payments of $45,000 which one of them planned to use to open an appliance store. They also suggested that the Americans were better suited to an operation in the United States and cajoled one of them into casing the New York Stock Exchange for a possible bombing—a "plot" that they never had any intention of carrying out, according to the testimony of one of them. The American did do a walk around the target, and then, several months later, submitted a one-page report on his adventure consisting of information that could have been gotten from Google Earth and from tourist brochures. His handlers were unimpressed.[76]

In his June 2013 testimony, Joyce said identification in the case was made not through 215, but through "702 authority."[77] At the same time, he raised interest, and then eyebrows, by dramatically proclaiming this to be a case "that was in the very initial stages of plotting to bomb the New York Stock Exchange." However, when asked whether the plot was "serious," Joyce deftly dodged the issue: "I think the jury considered it serious because they were all convicted." As it happens, there were no jury trials: the three men all pleaded guilty and then only to providing support to terrorism, not to the NYSE plot (such as it was). According to another official, FBI Deputy Director Joyce "misspoke."[78]

---

[76] Mark Morris, *Al-Qaeda Bunco Artist Rolls Terrorist from KC*, KANSAS CITY STAR, June 29, 2013, http://www.kansascity.com/news/local/article322244/Al-Qaeda-bunco-artist-rolls-terrorist-from-KC.html; Mark Morris, *KC Terrorist Supported Plan to Bomb New York Stock Exchange, FBI Tells Congress*, KANSAS CITY STAR, June 18, 2013, http://www.kansascity.com/2013/06/18/4299721/kc-terrorist-supported-plan-to.html.

[77] House Select Intelligence Committee Holds *Hearing on Disclosure of National Security Agency Surveillance Programs* (June 1, 2013) (transcript available at https://www.fas.org/irp/congress/2013_hr/disclosure.pdf); Ken McCarthy, *NSA Chief Says Exposure of Surveillance Programs Has 'Irreversible' Impact*, THE GUARDIAN (June 18, 2013), http://www.theguardian.com/world/2013/jun/18/nsa-chief-house-hearing-surveillance-live.

[78] Brian Ross, Aaron Katersky, James Gordon Meek, & Lee Ferran, *NSA Claim of NYSE Thwarted Plot Contradicted by Court Documents*, ABC NEWS (June 19, 2013),

The third disclosed case involves an American who had done surveillance work (the value of which seems to have been fairly limited) for terrorist gunmen who killed 166 in a suicidal rampage in Mumbai, India, in 2008. He was later arrested as he was engaged in a plot to do terrorist damage in Denmark, a plot that was beset by many planning and financial difficulties at the time. According to *ProPublica* reporter Sebastian Rotella who has done extensive research and reporting on the case, British intelligence already had the American under surveillance—suggesting that the Danish enterprise would never have been allowed to be carried out. The arrest resulted from a tip from the British, not from NSA intercepts. It does appear, however, that previously stored NSA intercepts, presumably from the 702 program, aided in building the legal case against the man.[79]

Only the fourth disclosed case involves a serious potential for terrorism within the United States. This was the Zazi case of 2009 in which three Afghan-Americans received training in Pakistan and then returned to the United States plotting to set off bombs on the New York subway system.

Joyce testified that a connection was made through "702 authority."[80] But, as Justin Heilmann points out in a study of the episode and as others have more recently noted, the plot in the United States does not appear to have been disrupted so much by NSA data-dredgers but by standard surveillance procedures implemented after the British provided a hot tip about Zazi based on his e-mail traffic to a known overseas terrorist address that had long been under surveillance.[81] At that point, US authorities had good reason to put the

---

http://abcnews.go.com/Blotter/nsa-claim-thwarted-nyse-plot-contradicted-court-documents/story?id=19436557.

[79] Sebastian Rotella, *Did NSA Surveillance Help Thwart Plotter of Mumbai Attack?,* FRONTLINE (June 12, 2013), www.pbs.org/wgbh/pages/frontline. *See also* Nick Gillespie, *Do the Zazi and Headley Arrests Prove the Power of NSA Total Surveillance?,* REASON.COM (June 13, 2013), http://reason.com/archives/2013/06/13/zazi-headley-feinstein-nsa. Joyce testified that the terrorist operative was uncovered "through 702 coverage of an al-Qaeda-affiliated terrorist." *Coverage of the NSA Hearings on Capitol Hill* (CNN Television Broadcast June 18, 2013) (transcript available at http://transcripts.cnn.com/TRANSCRIPTS/1306/18/cnr.05.html).

[80] *Id.*

[81] Justin Heilman, *Case 28: Zazi, in* TERRORISM SINCE 9/11: THE AMERICAN CASES, *supra* note 4, 347-55. More recent: Ben Smith, *Public Documents Contradict Claim Email Spying Foiled Terror Plot*, BUZZFEED (June 7, 2013), http://www.buzzfeed.com/bensmith/public-documents-contradict-claim-email-spying-foiled-terror. British tip: *British Spies Help Prevent al Qaeda-inspired Attack on New York Subway*, TELEGRAPH (Nov. 9, 2009),

plotters on their radar and as Senator Ron Wyden has pointed out, "the government had all the information it needed to go to the phone company and get an individual court order."[82] Having NSA's mega-data collection might have been helpful, but it seems scarcely to have been required.

Actually, it is not clear that even the tip was necessary. Given the perpetrators' limited capacities, it is questionable whether the plot would have ever succeeded. For example, the plotters foolishly called attention to themselves by using stolen credit cards to purchase large quantities of potential bomb material thereby guaranteeing that the sales would be scrutinized and security camera information preserved. Moreover, even with his training and a set of notes at hand, Zazi, described by a step-uncle as "a dumb kid, believe me," *still* apparently couldn't figure it out, and he frantically contacted his overseas trainer for help several times. Each of these communications was "more urgent in tone than the last," according to court documents.[83] It was these communications that alerted the authorities.

When presenting his four cases at the Congressional hearings in June 2013, Alexander explained that he couldn't make the details of all the cases on his secret list public because "If we give all those out, we give all the secrets of how we're tracking down the terrorists as a community, and we can't do that."[84] The remaining 50 will remain shrouded in secret, presumably because it is believed that discussing them publicly would result in damage, perhaps even grave damage, to

---

http://www.telegraph.co.uk/news/worldnews/northamerica/usa/6529436/British-spies-help-prevent-al-Qaeda-inspired-attack-on-New-York-subway.html. It is conceivable that the 702 program, PRISM, played a role in this process, but is not at all clear that this is so or that, if so, its role was necessary. For a discussion, see Dan Amira, *Did Controversial NSA Spy Programs Really Help Prevent an Attack on the Subway?,* N.Y. MAG. (June 10, 2013), http://nymag.com/daily/intelligencer/2013/06/nsa-prism-zazi-subway-feinstein-rogers-phone.html. Alexander has said that 702 was "critical," but that 215 was not essential to the case: McCarthy, *supra* note 77. *See also* Peter Finn & Greg Miller, *How an E-mail Address Disrupted Plots in Britain and U.S.,* WASH. POST, June 18, 2013, http://www.washingtonpost.com/world/national-security/how-a-shared-e-mail-address-disrupted-plots-in-britain-and-us/2013/06/18/ebb023c4-d84b-11e2-a016-92547bf094cc_story.html; MATT APUZZO & ADAM GOLDMAN, ENEMIES WITHIN: INSIDE THE NYPD'S SECRET SPYING UNIT AND BIN LADEN'S FINAL PLOT AGAINST AMERICA 53-55 (2013); Gillespie, *supra* note 79; Dilanian, *supra* note 72.

[82] Nakashima, *supra* note 60. *See also* Finn & Miller, *supra* note 81.

[83] John Mueller, *Mueller on the Zazi Case: 'This is It,'* INFORMED COMMENT (Nov. 4, 2009), http://www.juancole.com/2009/11/mueller-on-zazi-case-this-is-it.html.

[84] *NSA Chief Expected To Reveal New Terror Plots; House Intelligence Committee Hearing on Surveillance* (CNN Television Broadcast June 18, 2013) (transcript available at http://edition.cnn.com/TRANSCRIPTS/1306/18/cnr.03.html).

national security. Accordingly, we will never be able to examine them in our "healthy" debate on the issue of NSA surveillance.

Absent such information and keeping in mind the impressive record of dissembling that NSA has so far amassed, it does seem to be a reasonable suspicion—supported by the public comments of Senator Leahy—that the four cases discussed represent not a random selection from the list, but the best they could come up with. If that it so, the achievements of 215 do seem to be decidedly underwhelming.

In this regard, one could also examine that set of case studies of the 54 post-9/11 plots that have come to light by Islamist terrorists to damage targets in the United States.[85] Since these have resulted in public arrests and trials, there is quite a bit of information available about them. Overall, where the plots have been disrupted, the task was accomplished by ordinary policing methods. The NSA programs scarcely come up at all.

At the June 2013 hearings, one committee member, Representative Jim Himes of Connecticut, noting that his constituents were mainly concerned about 215, tried to get Alexander and Joyce to indicate how many plots would have been carried out but for that program. After some evasive answers, Himes, out of time, ended by expressing his "hope" that "you'll elucidate for us specifically case by case how many stopped terrorist attacks" the 215 program was "essential to."[86] Leahy's comments suggest that the answer to that question is perilously close to zero.[87]

IV. TERMINATING 215

It certainly appears, then, that any benefit of the 215 metadata program is very limited and is considerably outweighed by its cost, even assuming that the unknown, and perhaps unknowable, cost figure is quite small. The program would very likely fail a full cost-benefit analysis handily even only minimally taking into consideration

---

[85] TERRORISM SINCE 9/11: THE AMERICAN CASES, *supra* note 4.

[86] *House Select Intelligence Committee Holds Hearing on Disclosure of National Security Agency Surveillence Programs* (June 18, 2013) (transcript available at https://www.fas.org/irp/congress/2013_hr/disclosure.pdf).

[87] This conclusion is also supported by comments by Senator Ron Wyden in his keynote speech at the Cato Institute program, *NSA Surveillance: What We Know; What to Do About It* (Oct. 9, 2013) (video available at www.cato.org/events/nsa-surveillance-what-we-know-what-do-about-it). *See also* Justin Elliott, *Claim on 'Attacks Thwarted' by NSA Spreads Despite Lack of Evidence,* PROPUBLICA (Oct. 23, 2013), http://www.propublica.org/article/claim-on-attacks-thwarted-by-nsa-spreads-despite-lack-of-evidence.

privacy and civil liberties concerns. Representative Adam Schiff has done his own "on net" assessment. Even if the program is "occasionally successful," he concludes, "there's still no justification that I can see for obtaining that amount of data in the first place."[88] Some officials have in fact acknowledged that the case for 215 is "less compelling" and "harder to make."[89]

Although the cost of the 215 program remains classified, it is possible to calculate how much that cost would have to be for the program to be cost-effective. Even making some generous assumptions about its effectiveness, the program would be cost-effective only if its full price tag (including all the cost considerations arrayed above) is less than $33.3 million per year.[90] (The full NSA budget, for reference, is about $10 billion.) It is difficult to quantify the value of privacy, but it seems likely that considerably more than 33 million Americans would value their privacy enough to pay $1 a year to have their privacy shielded from NSA 215 surveillance.

In the past, NSA has actually closed down a privacy-invading program that had little demonstrable value in foiling terrorist plots—though not without characteristic dissembling. James Bamford reports that the agency had a nationwide program to store e-mail and Internet metadata in bulk for years. It was ended in 2011 for "operational and resource reasons," according to the director of national intelligence. But, notes Bamford, a statement issued in 2013 by senators Ron Wyden and Mark Udall contends that the real reason the program was shut down was that the NSA was "unable" to prove the usefulness of the operation. "We were very concerned about this program's impact on Americans' civil liberties and privacy rights," they said, "And we spent a significant portion of 2011 pressing intelligence officials to provide evidence of its effectiveness. They were unable to do so, and the program was shut down that year." The senators added, "It is also important to note that intelligence agencies

---

[88] Nakashima, *supra* note 60.

[89] Finn & Miller, *supra* note 81.

[90] It is assumed in this estimation that the 215 program is vital—is necessary to—the disruption of one plot every four years that, if successfully carried out, would result in the detonation of a very large improvised explosive device inflicting extensive damage to life and property costing $1 billion. This would be much larger than the car bomb that failed to detonate at Times Square in 2010. As noted, the 215 program has never done so in the past. Also assumed is that the chance the terrorist bomb would actually be successfully detonated in the undisrupted plot is 20 percent. On the (rather low) IED success rate for terrorists, see Matthew Grant & Mark G. Stewart, *A Systems Model for Probabilistic Risk Assessment of Improvised Explosive Device Attacks*, 5 INT'L J. OF INTELLIGENT DEF. SUPPORT SYS. 1, 75-93 (2012).

made statements to both Congress and the [FISA court] that significantly exaggerated this program's effectiveness. This experience demonstrates to us that intelligence agencies' assessment of the usefulness of particular collection program—even significant ones—are not always accurate."[91]

It seems likely that "on net" (as the President puts it) the highly controversial 215 program could safely be retired for "operational and resource reasons" with little or no negative consequences to security. If the 215 program has done little (and probably nothing) special to prevent or disrupt terrorist attacks in the United States, and if we are now having a healthy debate about the NSA programs, it seems reasonable to suggest that, even without full information about how the program costs, we are paying too much.

And, just possibly, there are other elements in the vast intelligence and policing empire spawned in panic and in unseemly haste after 9/11 that might also be retired. In a major speech on the NSA controversy in January 2014, President Obama stated, "One thing I'm certain of. This debate will make us stronger."[92] The speech contained no suggestion about honoring the man responsible for getting the debate going, and therefore for strengthening the United States. However, if Snowden's debate does lead to systematic efforts to evaluate the huge increases in homeland security that have taken place since 2001, it will prove to be a most desirable development.

---

[91] Bamford, *supra* note 25. *See also* LIBERTY AND SECURITY IN A CHANGING WORLD, *supra* note 10, at 96. Further information at Press Release from Wyden, Udall on the Disclosure of Bulk Email Records Collection Program, (July 2, 2013) (*available at* http://www.wyden.senate.gov/news/press-releases/wyden-udall-statement-on-the-disclosure-of-bulk-email-records-collection-program), which also includes this observation: "We believe that the broader lesson here is that even though intelligence officials may be well intentioned, assertions from intelligence agencies about the value and effectiveness of particular programs should not simply be accepted at face value by policymakers or oversight bodies....It is up to Congress, the courts and the public to ask the tough questions and press even experienced intelligence officials to back their assertions up with actual evidence, rather than simply deferring to these officials' conclusions without challenging them."

[92] Remarks by the President on Review of Signals Intelligence, Department of Justice (Jan. 17, 2014) (*available at* http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence).